Journal of Advances and Scholarly Researches in Allied Education
Vol. 21, Issue No. 5, July-2024, ISSN 2230-7540

DOI: https://doi.org/10.29070/2wffdw49

Check for updates

Analyzing the Security and Efficiency of Pairing-free Directed Signature Schemes on Elliptic Curve Cryptography

Sajitha V G [1] * , Dr. Dharmendra Saxena [2]

1. Research Scholar, Department of Mathematics, University of Technology, Jaipur, Rajasthan, India
sajithavg1981@gmail.com ,
2. Professor, Department of Mathematics, University of Technology, Jaipur, Rajasthan, India

Abstract: Communications have grown at an exponential rate throughout the modern period. The need of security in contexts with limited resources has been highlighted by applications such as online banking, personal digital assistants, mobile communication, smartcards, etc. With low key sizes and good security on par with other common public key techniques, elliptic curve cryptography (ECC) is an ideal tool for cryptography. ECC is a method of data encryption that relies on keys. Encryption and decryption are the main focusses of ECC, which relies on public and private key pairs. The Elliptic Curve Discrete Logarithm Problem (ECDLP) is a computationally intractable inverse process that gives rise to ECC methods, which are based on scalar multiplication of elliptic curve points. An exhaustive examination of the difficulties in creating ECC-based systems was accompanied by an assessment of current ECC solutions. Domain parameter selection, scalar multiplication, point multiplication, elliptic curve generation, key generation, key size selection, security measures, applications, and so on are some of the difficulties highlighted in the study.

Keywords: crypto-graphic, Blind signature, elliptic curve, storage capacity, cryptosystem

X

INTRODUCTION

One of the most basic and practical cryptographic primitives, a digital signature ensures the veracity and immutability of digital messages. In order for digital signatures to be used in practical contexts, they must take into account various aspects and attributes to ensure they are suitable for various purposes. A wide variety of digital signature schemes, each with its own set of advantages and disadvantages, have been proposed in the literature for use in various cryptographic contexts, including the more conventional public key infrastructure (PKI) (Differ and Hellman, 1976) and identity-based cryptosystems (Shamir, 1984).

Certificates issued by certification authorities (CAs) and including information about the user's identity and legality serve as the foundation of conventional public key infrastructure (PKI) security. However, there are additional storage, calculation, and communication expenses associated with certificate administration. In contrast to conventional PKI, the Identity Based Cryptosystem (IBC) (Shamir, 1984) may verify the legitimacy of a public/private key pair without the need of a certificate. The system relies on a trusted third party called a Private Key Generator (PKG) to produce secret keys, while the public key of a user is obtained from their identification. There is an underlying key escrow issue with IBC, even if it systematically removes the need for certificates. A new technique known as certificateless public key cryptography (CL-PKC) was later proposed by Al-Riyami and Paterson (2003). You may think of this method as a hybrid of regular PKI and ID-PKC as it avoids the key escrow issue and doesn't need certificates.

To sign sensitive communications more effectively, it is best to use a mix of directed signature approach and proxy signature, which combines the best features of both. Take this scenario into consideration: Bob now has access to his medical history thanks to Doctor Alice's digital signature on a hospital document. By designating Doctor Charlie as his proxy, Alice may transfer his signature authority to him. After that, Bob may independently confirm these signs with others who are unaware of his disease. Otherwise, his disease status would be revealed. Bob will also have to show the other doctor that his medical records are legitimate after some time has passed if he wants to get well. Also, when Bob isn't available to do so, Doctor Charlie is equally capable and responsible for acknowledging these medical documents. Several directed proxy signature systems have been suggested in the literature [27, 28, 29] in response to the case mentioned above. In these systems, a third party acts as a proxy signer, sending a digital signature to a trusted verifier in place of the original signer. The designated verifier has the authority to personally confirm the authenticity of the proxy signature and persuade any third party to accept it.

Additionally, bilinear pairings over elliptic curves are used in the construction of all the directed proxy signature schemes that have been mentioned above. When compared to the evaluation of a scalar multiplication in an elliptic curve, the pairing process is more costly and time-consuming. As an example, the degree of security provided by RSA with 2048-bit keys and ECC with 224-bit keys are same. Therefore, ECC has gained popularity because to its ability to provide increased security with reduced key sizes. Computational and communicational efficiency, storage capacity, and bandwidth efficiency are all enhanced by this lower key size. A single pairing operation has a 20-fold evaluation compared to scalar multiplication. Regarding this matter, designing the signature scheme without using bilinear pairing operations is necessary to further enhance the computing efficiency of directed proxy signature schemes. Because of this, we set out to create an ID-based pairing-free directed proxy signature system.

From bilinear pairings in the random oracle model, the first efficient ID-based directed signature scheme (ID-DS) was developed. An ID-DS method devoid of random oracles was suggested in 2009. Also that year, put forth a plan to use bilinear pairings to improve ID-DS performance. A hyper elliptic curve directed signature system based on ID was introduced in 2012 and shown to be efficient. Put forth the first pairing-based certificateless directed signature technique in 2011.

LITERATURE REVIEW

Gayathri, N. B. et.al. (2018). Under a standard signature technique, everyone may check whether a signer's signature is legitimate. Some uses, such as signatures on medical records or tax information, do not want the signed message to be publicly verifiable because of the sensitive nature of the information it contains. The idea of directed signature was developed to fulfil this need. The signer has control over the verification ability in a directed signature scheme, a kind of signature method. In various cryptographic contexts, several directed signature techniques have been suggested, the majority of which use bilinear pairings over elliptic curves. However, bilinear pairing computation is too costly. That is why pairing-based methods aren't very practical and inefficient. Our proposal for a pairing-free certificateless directed signature technique aims to enhance computational and communicational efficiency in this work. Assuming the discrete logarithm issue for elliptic curves is difficult, the suggested approach is shown to be safe in the random oracle model. After comparing our plan to well-known existing schemes, we found that the suggested scheme is more efficient according to the efficiency study.

Gayathri, N. B. & Rao, R. et.al (2017). Digital signatures are crucial to the security of today's pervasive and irreplaceable electronic communication. The use of digital signatures has grown swiftly in tandem with developments in lattices, pairings, and elliptic curves in mathematics. Ellipstic curve cryptographic techniques are still the gold standard for many security-related tasks because of their great efficiency and robust security features. There is a growing interest in efficient community in pairing free signature techniques on elliptic curves. Many different kinds of digital signature techniques have developed throughout the years to address various use cases. Directed signature technique is one example of such a version. In a directed signature, the signer has complete control over the signature's verification capability. In this case, only a designated verification can confirm the signature's authenticity, and no one knows who that verifier is. When the recipient's privacy is paramount, as in a health or tax bill, directed signature methods are the way to go. Here we provide an efficient and secure Identity (ID) based directed signature (IDBDS) approach over elliptic curves that does not need pairing. This is the only technique that we are aware of that addresses directedness in a pairing-free environment in an ID-based context. We demonstrate its safety by use of a random oracle model, supposing that the Elliptic Curve Discrete Logarithm Problem (ECDLP) is difficult. Efficiency research reveals that our method outperforms all other comparable schemes when compared to well-known current schemes.

Gayathri, N. B. et.al. (2019). Applications for monitoring infrastructure, earthquakes, environments, remote healthcare, etc., have emerged as a result of recent developments in wireless communication technology. Where sensor nodes dynamically join the internet and use it to cooperate and complete tasks, we may combine Wireless Sensor Networks (WSNs) with the Internet of Things (IoT) in these applications. Internet of Things (IoT) terminals allow for the constant monitoring and collection of physiological data via wireless medical sensor nodes, which are an integral part of an e-healthcare system. There has been little discussion of signature systems in the literature as a means to circumvent sensors' communication and processing restrictions and achieve privacy in healthcare wireless medical sensor networks (HWMSNs). Having said that, the majority of these schemes are vulnerable to a variety of assaults. Therefore, in this study, we suggested a pairing-free aggregate signature technique for HWMSNs in a certificateless system to guarantee the confidentiality of medical records. As a means of lowering the computational complexity and transmission overhead associated with data transfer, we make use of the aggregation approach in certificateless systems without pairings. The performance evaluation demonstrates that the suggested system is more efficient, and our approach accomplishes complete aggregation to enhance communicational efficiency.

Wei, Qian et.al. (2009). No one wants their private information—like which group they want to join, who manages the group, and who gives out admittance tokens—out in the open and hence vulnerable to attackers, therefore they enter confidential groups. The privacy of the incoming member cannot be effectively protected by the group key initial distribution based on basic signature as anybody possessing the appropriate public key may verify the basic signature. We provide a directed signature strategy for confidential group communication that is based on the elliptic curve ElGamal cryptosystems and applies it to the group key initial distribution. The experimental results demonstrate that our directed signature scheme is statistically indistinguishable from the digital signature scheme in terms of computation cost when compared to the elliptic curve ElGamal scheme. This means that the group key initial distribution based on our scheme not only efficiently protects the entering member's privacy but also saves computation resources.

Gayathri, N. B. et.al. (2019). Applications for monitoring infrastructure, earthquakes, environments, remote healthcare, etc., have emerged as a result of recent developments in wireless communication technology. Where sensor nodes dynamically join the internet and use it to cooperate and complete tasks, we may combine Wireless Sensor Networks (WSNs) with the Internet of Things (IoT) in these applications. Internet of Things (IoT) terminals allow for the constant monitoring and collection of physiological data via wireless medical sensor nodes, which are an integral part of an e-healthcare system. There has been little discussion of signature systems in the literature as a means to circumvent sensors' communication and processing restrictions and achieve privacy in healthcare wireless medical sensor networks (HWMSNs). Having said that, the majority of these schemes are vulnerable to a variety of assaults. Therefore, in this study, we suggested a pairing-free aggregate signature technique for HWMSNs in a certificateless system to guarantee the confidentiality of medical records. As a means of lowering the computational complexity and transmission overhead associated with data transfer, we make use of the aggregation approach in certificateless systems without pairings. The performance evaluation demonstrates that the suggested system is more efficient, and our approach accomplishes complete aggregation to enhance communicational efficiency.

RESEARCH METHODOLOGY

Method

A technique is suggested for creating a one-of-a-kind cryptographic key that is produced from the user's permanent fingerprints. Compared to the conventional cryptography system, the suggested method simplifies the process of generating crypto keys, thereby lowering the cost associated with wasted opportunities. Since storing the key in a database makes it more difficult to break or guess the cryptographic keys, they are instead generated directly from the fingerprint data. Positive outlooks on information security will be provided by biometrics, encryption, and data concealing. We put out a method for developing algorithms that are both highly secure and very efficient in terms of bandwidth and computing power. Although there are already a number of biometric systems that handle cryptography, the suggested figure print parameter based cryptographic key presents a new way to create cryptographic keys. This method, when used in MATLAB, may produce cryptographic keys of varying sizes with a negligible time complexity, making it ideal for use in real-time cryptography.

Design Details

Improving the picture, segmenting the image, and performing the final extraction are all steps in the image processing pipeline that make up minutiae extraction. Contrast stretching is what happens in histogram equalisation. We distribute intensity. The histogram of the fingerprint picture is narrow, as can be seen. To change an image's domain (from spatial to frequency), one uses Fast Fourier Transform. displays both the pre- and post-FFT effects. Image binarization is the process of converting greyscale images to binary images. Following the procedure, the furrows will appear white, while the ridges will be emphasised with black.

DATA ANALYSIS

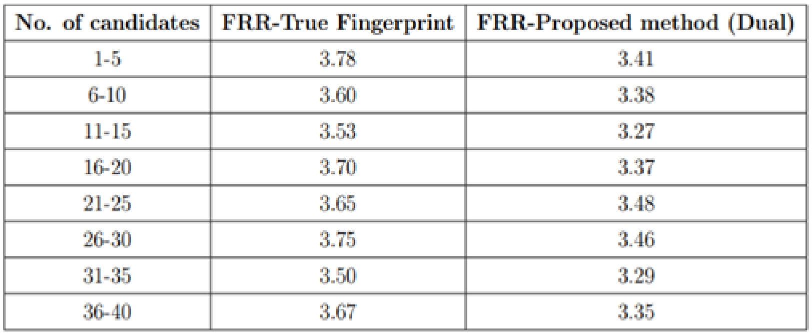
Analysis

In our experiment, we used fingerprint pictures sourced from the publicly accessible FVC2002 database [14]. This collection includes 40 distinct greyscale fingers with 8 impressions per finger, for a total of 320 fingerprints (40 ∏ 80= 80). The results of the experiment show that the suggested method is safe, quick, dependable, reversible, and attack-proof. Both Table 1 and Table 2 show the experimental outcomes of the suggested method. The False Acceptance Rate (FAR) and the False Rejection Rate (FRR) are the metrics that are used for assessment. The FRR measures how often authorised individuals are denied entry.

False Rejection Rate = Number of imposter rejected / Total number of imposter trials

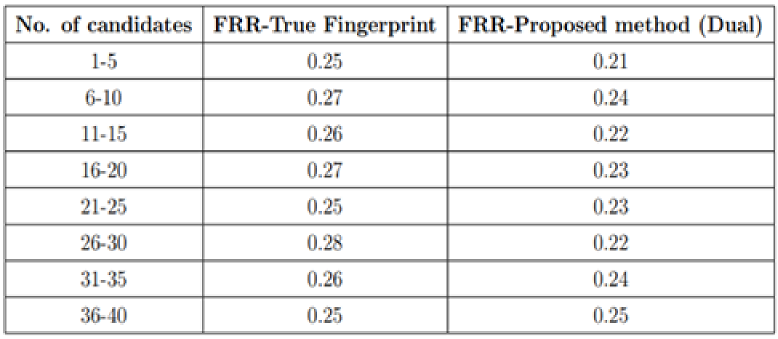
False Acceptance Rate = Number of imposter accepted / Total number of imposter trials

Table.1: "FRR(%) for various users"



No. of candidates	FRR-True Fingerprint	FRR-Proposed method (Dual)
1-5	3.78	3.41
6-10	3.60	3.38
11-15	3.53	3.27
16-20	3.70	3.37
21-25	3.65	3.48
26-30	3.75	3.46
31-35	3.50	3.29
36-40	3.67	3.35

Table.2: "FAR(%) for various users"



No. of candidates	FRR-True Fingerprint	FRR-Proposed method (Dual)
1-5	0.25	0.21
6-10	0.27	0.24
11-15	0.26	0.22
16-20	0.27	0.23
21-25	0.25	0.23
26-30	0.28	0.22
31-35	0.26	0.24
36-40	0.25	0.25

Evaluation based on FRR and FAR

We have taken into account user clusters to assess the efficacy of dual fingerprint.The production of keys is the subject of much investigation using both real and dual fingerprints. In comparison to the genuine fingerprint technique, the False Acceptance Ratio and False Rejection Ratio of the dual fingerprint approach are lower (Figures 1 and 2).

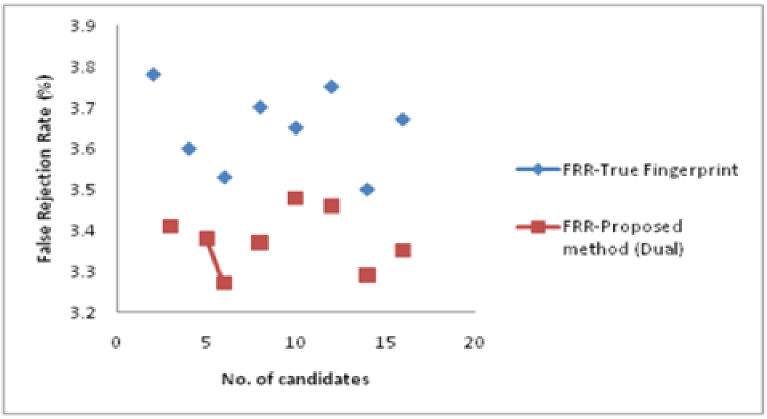


Figure 1: False Rejection Ratio (True Fingerprint vs Dual Fingerprint)

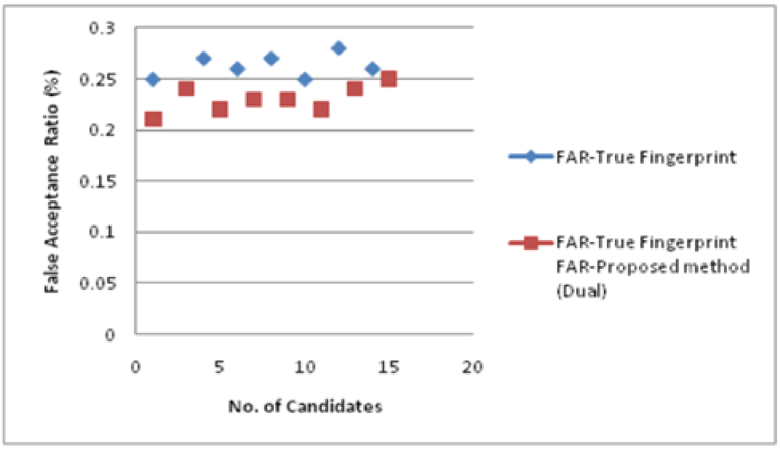


Figure 2: False Acceptance Ratio (True Fingerprint vs Dual Fingerprint)

Secure Load Balancing for Fog-IoT Middleware using ECC Based Authentication

In terms of processing speed, memory, secondary storage, device size, networking capabilities, energy availability, and so on, IoT devices are severely constrained. Despite the devices' minimal resources, the Internet of Things (IoT) network need the same level of security services, if not more, as a traditional network due to the hostile environments in which they are placed. The level of secrecy, authenticity, and integrity that an IoT network must provide is closely related to the security requirements of the applications it supports. Authentication is especially important for the Internet of Things (IoT) [119] since users must have faith in the gadgets that make up an IoT network for it to perform properly.

CONCLUSION

An approach to data encryption known as Elliptic Curve Cryptography (ECC) uses keys. When it comes to encrypting and decrypting online traffic, ECC is all about public-private key pairs. A strong alternative to RSA, ECC is a method of cryptography. It uses the theory of elliptic curves to create a secure connection between public key encryption key pairs.

The ECC method for public key cryptography differs from RSA in that it relies on the algebraic structure of elliptic curves over finite fields. Keys generated by ECC are therefore mathematically more difficult to break. This is why ECC is seen as a more secure alternative to RSA and the next gen of public key cryptography.

References

1. Gayathri, N. B. & Gowri, T. & Rao, R.R.V. & Reddy, Vasudeva. (2018). Efficient and secure pairing-free certificateless directed signature scheme. Journal of King Saud University - Computer and Information Sciences. 33. 10.1016/j.jksuci.2018.02.016.

2. Gayathri, N. B. & Rao, R. & deva, P Vasu. (2017). Efficient and Provably Secure Pairing Free ID-Based Directed Signature Scheme. 28-38. 10.1007/978-981-10-6898-0_3.

3. Gayathri, N. B. & Gowri, T. & Kumar, P. & Mohammad, Zia Ur Rahman & Reddy, Vasudeva & Lay-Ekuakille, Aimer. (2019). Efficient and Secure Pairing-Free Certificateless Aggregate Signature Scheme for Healthcare Wireless Medical Sensor Networks. IEEE Internet of Things Journal. PP. 1-1. 10.1109/JIOT.2019.2927089.

4. Wei, Qian & Shao, Huiying. (2009). A directed signature scheme and its application to group key initial distribution. ACM International Conference Proceeding Series. 403. 265-269. 10.1145/1655925.1655972.

5. Gayathri, N. B. & Gowri, T. & Kumar, P. & Mohammad, Zia Ur Rahman & Reddy, Vasudeva & Lay-Ekuakille, Aimer. (2019). Efficient and Secure Pairing-Free Certificateless Aggregate Signature Scheme for Healthcare Wireless Medical Sensor Networks. IEEE Internet of Things Journal. PP. 1-1. 10.1109/JIOT.2019.2927089.

6. X. Zhu, S. Jiang, L. Wang and H. Li, “Efficient privacy preserving authentication for vehicular ad hoc networks,” IEEE transactions on vehicular technology, vol. 63, no. 2, pp. 907-919, 2014.

7. F. Wang, Y. Xu, H. Zhang, Y. Zhang and L. Zhu, “2FLIP: A two factor lightweight privacy preserving authentication scheme for VANET” IEEE transactions on vehicular technology, vol. 65, no. 2, pp. 896-910, 2016. [5]

8. X. Lin, X. Sun, P. H. Ho, and X. Shen, “GSIS: a secure and privacy-preserving protocol for vehicular communications,” IEEE Transactions on Vehicular Technology, vol. 56, no. 6, pp. 3442– 3456, 2007.

9. Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, “An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications,” IEEE Transactions on Vehicular Technology, vol. 59, no.7, pp. 3589–3603, 2010.

10. H. Lu, and L. Jie, “Privacy-preserving authentication schemes for vehicular ad hoc networks: a survey,” Wireless Communications and Mobile Computing, vol. 16, no. 6, pp. 643- 655, 2016. [18]

11. Y. Wang, H. Zhong, Y. Xu, J. Cui, and F. Guo, “Efficient extensible conditional privacypreserving

authentication scheme supporting batch verification for VANETs," Security and communication networks, vol. 9, no.18, pp. 5460- 5471, 2016

12. S. F. Tzeng, S. J. Horng, T. Li, X. Wang, P.H. Huang, and M. K. Khan, "Enhancing security and privacy for Identity-based batch verification scheme in VANET," IEEE transactions on vehicular technology, vol. 66, no. 4, pp. 3235- 3248, 2017. [20]
13. X. Hu, J. Wang, H.Xu, Y.Liu, and X. Zhang "Secure and pairing-free Identity-based batch verification scheme in vehicle ad-hoc networks, " in Proc. of ICIC-2016,Part III, LNAI 9773, 2016, pp. 11-20.
14. J. Cui, J. Zhang, H. Zhong, and Y. Xu, "SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter," IEEE transactions on vehicular technology, vol. 66, no.11, pp. 10283-10295, 2017.
15. Al-Riyami, S. S., Paterson, K.G., Certificateless Public key Cryptography. LNCS, vol. 2894, pp. 452-473. 2003